SCIENTIFIC JOURNAL OF MARITIME RESEARCH [POMORSTVO]
University of Rijeka FACULTY OF MARITIME STUDIES

https://doi.org/10.31217/p.39.2.6

Cybersecurity Applications in the Maritime Industry: A Scientometric Approach

Burcu Yilmaz

Kayseri Üniversitesi, Uygulamalı Bilimler Fakültesi, Uluslararası Ticaret ve Lojistik Bölümü, Mevlana Mahallesi, 15 Temmuz Yerleşkesi, Kümeevler, 38280 Talas / KAYSERİ – Türkiye, e-mail: burcukaya107@gmail.com

ARTICLE INFO

Review article
Received 11 February 2025
Accepted 5 May 2025

Key words:
Maritime
Shipping
Cybersecurity
Cyber risk
Bibliometric analysis

ABSTRACT

The maritime industry, which holds significant importance for international logistics operations and global trade, is increasingly exposed to cybersecurity risks in this era of accelerating digitalization. In this context, cybersecurity research conducted within the maritime sector is crucial in maintaining international trade, preventing economic losses, and effectively managing global supply chains. In this regard, the primary objective of this study is to examine research on cybersecurity applications in the maritime field using the scientific mapping method and to identify prominent topics and themes. Accordingly, a search was conducted in the Web of Science database using maritime-related keywords in combination with the terms "cybersecurity," "cyber risk," "cyber threats," or "cyber risk management." Covering the period from 2014 to December 2024, including early-access publications slated for 2025, 248 studies incorporating maritime concepts and these cybersecurity-related terms were analyzed using the R programming language. The analysis results indicate that research in this field began in 2014 and that there has been a notable increase in the number of studies conducted since 2018. The findings reveal that the most frequently used keywords in this field include "model," "cybersecurity," "performance," and "safety." Additionally, *the Journal of Marine Science and Engineering* stands out as the journal that has published the highest number of studies and received the most citations in this domain. The top three countries with the highest number of publications in this field are Norway, the United Kingdom, and the United States, respectively. Furthermore, the prominent thematic focus identified in the research is *collision-avoidance navigation*. These findings are significant for researchers, policymakers, and practitioners, as they also contribute to developing recommendations for future studies.

1 Introduction

Maritime transportation holds a critical position for all industries, as it ensures the delivery of various resources to production centers and facilitates the supply of energy required for manufacturing. Since a significant portion of international trade is conducted through maritime transportation, these activities substantially impact economic development [1,2]. More than 80% of global trade volume is carried out via sea routes, which in turn has profound implications for food security, energy resources, and the global economy [3]. As a result of Industry 4.0, advanced technological developments have been rapidly integrated into all sectors. With the increasing adoption of these advanced technologies, the maritime industry is also undergoing a transformation driven by the innovations they introduce. However, integrating Industry 4.0 technologies, particularly through the Internet of Things (IoT), has interconnected critical maritime systems, thereby increasing their vulnerability to cyberattacks. As digital technologies are incorporated into the sector, the risks associated with these innovations are also escalating, posing significant threats to the execution of operational processes [4]. To ensure efficient operations management, onboard computers and software systems are extensively utilized [5 (p. 2)]. With the increasing use of digital tools, the risk of cyber threats is also rising, leading to significant security vulnerabilities in the maritime industry. Cyberattacks targeting the maritime sector create international

security concerns and disrupt the supply chains essential for global production, resulting in substantial financial losses [6 (p. 174)]. Therefore, taking precautionary measures and developing solutions to address potential cybersecurity issues in the maritime industry are critical for establishing secure trade routes and ensuring operational efficiency in maritime transportation.

Given the pervasive cybersecurity challenges, it is essential to systematically analyze the evolution and scope of research in this domain. Adopting a scientometric approach offers a novel and objective method to measure trends, identify research gaps, and uncover new patterns in maritime cybersecurity studies, which case analysis and traditional reviews such as systematic reviews may overlook. This comprehensive analysis is particularly essential for informing future research directions and policy-making, as it provides clear, evidence-based insights into the dynamic and interdisciplinary nature of the field. In this context, the quantitative assessment of scientific studies on maritime cybersecurity is considered essential for the more effective development of cybersecurity strategies in the maritime sector and ensuring that sector-specific policies are grounded in scientific evidence.

This study aims to assess current trends and research gaps in the literature concerning cybersecurity applications in the maritime sector and to provide recommendations for future studies based on the findings of a bibliometric analysis. Considering the growing interest in cyber risks alongside the integration of digital technologies into the maritime sector, it has been identified that bibliometric studies on this subject remain limited in the existing literature. Rather than claiming to fully address this gap, the present study seeks to contribute to the ongoing academic conversation by providing a detailed and structured analysis of existing research and by highlighting key themes and underexplored areas. In this regard, it is hoped that the study will serve as a useful reference point for future investigations in the field.

Bibliometric studies in this field primarily employ systematic literature review and bibliometric techniques, drawing data predominantly from the Scopus database. Some studies also utilize data from the WOS database, offering a complementary perspective. It is important to acknowledge the limitations inherent in the selected databases and tools. For example, while the Scopus database generally offers broader coverage in terms of journals and subject areas, the WoS database is known for its rigorous indexing standards, which may lead to variations in article representation across fields. In this context, the Web of Science database was utilized as a primary source. Accordingly, various aspects of maritime cybersecurity research were analyzed using 248 scientific publications obtained from a search in the Web of Science database. These include the number of citations received over the years, frequently used keywords, keyword trends, the most prolific authors in this field, the most productive institutions, and international scientific collaborations. Furthermore, key topics and concepts in cybersecurity applications within the maritime sector were identified, and various recommendations for future research were provided.

2 Conceptual framework and literature review

Forecasts for the 2025–2029 period indicate that the global trade volume transported by sea will grow at an average annual rate of 2.4%, while container shipping is expected to expand by 2.7%. Increasing infrastructure investments, technological advancements, and initiatives aimed at reducing carbon emissions further enhance maritime transportation's significance in international trade [3].

In today's rapidly advancing technological landscape, the maritime sector is also undergoing a transformation driven by the innovations required by digital technologies. The integration of information and communication technologies (ICTs) with operational processes in maritime transportation enhances the efficiency of transport management [7 (p. 1)]. As of 2025, increasing geopolitical tensions in various regions pose significant risks to global maritime transportation. Key threats include piracy activities in the Indian Ocean and off the coast of East Africa, Israel's ongoing military interventions in the Mediterranean, the recent political collapse in Syria, potential Hezbollah interventions in supply chains affecting global logistics, and the ongoing Ukraine-Russia war in the Black Sea—all of which are critical factors that could impact international maritime trade [8]. Due to these tensions, cyberattacks targeting ships in maritime transportation are also likely to occur. In this context, ensuring cybersecurity in maritime transportation is of critical importance not only for maintaining seamless operational processes but also for enhancing international cooperation among countries to support the sustainability of global maritime trade.

With the increasing digitalization in the maritime industry, cybersecurity has emerged as a critical domain affecting the safety of ship operations and port services. In this context, current literature studies reveal the industry's principal cybersecurity vulnerabilities and offer solutions to security vulnerabilities. In particular, security weaknesses in ship navigation systems are among the common topics numerous studies address. These systems, often operating on outdated operating systems and unsupported software, become increasingly susceptible to external interventions [9,10]. Attacks targeting navigation systems may lead to the creation of false vessel positions, manipulation of ship routes, or even complete system shutdowns [11,12]. Therefore, strengthening cybersecurity practices in maritime operations has become essential to ensuring the uninterrupted continuity of ship-related processes.

Studies addressing the malicious use of the Automatic Identification System (AIS) demonstrate that this technology can be exploited for data transmission and as a command and control mechanism. Integrating malware via AIS can result in unauthorized access to ship systems and even a complete takeover [13]. On the other hand, Cyber Security Operations Centers (CSOCs) developed to detect and manage cyber threats can provide effective results with real-time monitoring and machine learning-based detection systems [14].

Beyond technical vulnerabilities, many studies emphasize the role of human factors in cybersecurity risks. Low levels of cybersecurity awareness among crew members represent a significant risk factor [11,14]. Accordingly, it is widely recommended that technical measures be complemented by training programs tailored to maritime staff and crew to raise awareness and preparedness [15].

Studies focusing on autonomous passenger ships indicate that traditional cybersecurity approaches are insufficient to address the complex risks associated with these new technologies. Defense-in-Depth strategies alone are considered inadequate; instead, flexible, threat-informed, and layered defense models are suggested [16]. In this regard, the same study proposes next-generation solutions, such as VPN tunnels, and highlights that non-IP-based communication protocols may render conventional security methods ineffective.

Moreover, the literature includes studies that analyze specific cybersecurity incidents to classify threat types and frequencies. For instance, an analysis of 46 incidents between 2010 and 2020 shows the prevalence of ransomware attacks, invoice fraud, and espionage activities in the sector. These attacks commonly target transportation companies, ports, and shipyards. Notably, the frequency of jamming and spoofing attacks has been reported to increase in geopolitically tense regions such as the Black Sea [17]. These cases illustrate that cyber threats in the maritime domain may also carry significant political dimensions. In addition, novel methodologies have been developed to assess risk in systems lacking historical data, offering new frameworks based on attacker motivation, opportunity, and capability [18].

These studies suggest a significant body of literature has emerged on maritime cybersecurity. However, this literature tends to concentrate on similar systems and threat types. There appears to be a relative lack of research on more advanced cyberattack scenarios and developing comprehensive defense mechanisms against such threats. In this regard, the growing need for multilayered security strategies encompassing ships, ports, shipyards, and autonomous systems stands out as a guiding direction for future research. Lastly, expanding research on human-machine interaction and field-based training programs could improve the readiness of both crew and port personnel against cyber threats. Studies addressing these areas are expected to contribute to both the theoretical development and practical application of maritime cybersecurity literature.

Table 1 Studies conducted in the field of Maritime cybersecurity

Author(s)	Domain	Key Findings
[9]	Cyber Risk Management in Ship Operations	As a result of a survey conducted with ship crew members, a total of 14 security vulnerabilities were identified, seven of which were classified as critical. It was determined that the Electronic Chart Display and Information System (ECDIS) was operating on the Windows XP Service Pack 2 operating system, which is no longer supported, making it an open target for attackers. A vulnerability was found in the Server Message Block (SMB) protocol that allows an attacker to execute arbitrary code remotely. Additionally, ECDIS was found to mishandle Remote Procedure Call (RPC) requests, posing another security risk. The system was also affected by multiple SMB-related vulnerabilities, enabling unauthenticated attackers to gain access to sensitive information—placing these issues among the critical vulnerabilities identified.
[11]	Maritime Cyber Risk Assessment	In the study, the MaCRA (Maritime Cyber-Risk Assessment) model conducts risk assessment along three dimensions: system vulnerabilities, attack feasibility, and attacker benefit. It was identified that navigation systems (GPS, AIS, ECDIS) may be vulnerable to cyberattacks; through AIS spoofing, fictitious vessels can be created, or the positions of existing vessels can be manipulated. The crew's low level of cybersecurity awareness contributes to increased human-related threats. Additionally, open ports and outdated software facilitate unauthorized access to ship systems by attackers. Attacks on cargo management systems may lead to the use of falsified documents, thereby increasing the risk of smuggling activities.
[14]	Cyber Threats in the Maritime Industry	A Cybersecurity Operations Center (CSOC) was developed to identify and mitigate the security risks arising from the digitalization of military and commercial vessels. Cyber threats were successfully identified through real-time threat monitoring and AI-assisted attack detection systems. The findings indicate that systems such as GPS, AIS, ECDIS, and onboard networks have become vulnerable to cyberattacks. Moreover, it was observed that when crew members and ship captains are informed about potential attacks, emergency measures can be implemented. Machine learning and signature-based threat detection systems have also been shown to enable the early detection of cyber incidents.

Author(s)	Domain	Key Findings
[12]	Cybersecurity Challenges in the Maritime Industry	The study sheds light on cybersecurity issues in the maritime sector. According to the findings, GPS spoofing—broadcasting false GPS signals—can cause vessels to report incorrect positions and alter their actual routes. GPS jamming can altogether disable a ship's navigation systems. The manipulation of AIS data may lead to the creation of fake vessels or the concealment of real vessel positions, thereby increasing the risk of collisions. Furthermore, it has been noted that ship engine systems, fuel management systems, and cargo handling systems are particularly vulnerable to cyberattacks.
[13]	Cybersecurity Vulnerabilities in the Maritime Industry	The study explains how the Automatic Identification System (AIS) can be exploited as a command and control mechanism in cyberattacks. The findings reveal that AIS messages can be misused to send instructions to vessels and deploy malicious software updates remotely. It was also found that hidden commands or malicious files can be embedded within AIS messages, allowing attackers to take control of ship systems. Additionally, AIS can be used to monitor network traffic and manipulate the vessel's navigational data.
[17]	Cyber Threats in the Maritime Industry	The study examines 46 cybersecurity incidents that occurred between 2010 and 2020 and identifies the most significant threats the maritime sector faces. The findings show that 25% of the attacks targeted shipping companies, with ransomware identified as the most common type of cyberattack in this domain. It was also revealed that shipbuilding yards and research centers are exposed to similar threats, and state-sponsored actors can target port systems. The study highlights the presence of large-scale and targeted espionage campaigns within the sector, including spear-phishing, hacking, and communication interception. IT systems onboard vessels were found to be vulnerable to ransomware attacks, while jamming and spoofing were reported as the most frequent forms of disruption, particularly in geopolitically sensitive areas such as the Black Sea. The findings also indicate that attackers attempt to gain financial advantage by altering account information or issuing fraudulent invoices.
[10]	Ship Cybersecurity	The study analyzes cybersecurity vulnerabilities in Electronic Chart Display and Information System (ECDIS) workstations used in paperless ship navigation. Security tests revealed that the DNS client running on ECDIS systems was outdated and exposed to known vulnerabilities, potentially allowing remote execution of malicious code. Additional vulnerabilities were identified in the Security Account Manager (SAM) and Local Security Authority (LSAD) components, which could enable an attacker to gain system access by impersonating an authorized user. The study concludes that the root causes of these vulnerabilities lie in using outdated operating systems and legacy communication protocols.
[18]	Cyber Threat Assessment and Risk Management in the Maritime Industry	This study develops a systematic approach for assessing cyber threats in systems that lack historical data on past security incidents. The findings indicate that a significant portion of threats are associated with the infiltration of ship systems by malicious software. Four key factors were identified to determine the likelihood of a system being attacked: the presence of threat actors, opportunities for attack, the tools required for execution, and attacker motivation. It was concluded that the maritime sector is frequently targeted by hacker groups and state-sponsored threat actors, with ransomware, financial gain, political objectives, and espionage identified as the primary driving motivations. Furthermore, the likelihood of cyberattacks is increased by factors such as remote access, maintenance updates, and existing system vulnerabilities.
[15]	Port Cybersecurity	The study employs an integrated cybersecurity risk assessment model. Within this framework, four distinct cyberattack scenarios were analyzed: remote access and data manipulation targeting the port information system, critical system update failure during a power outage, data leakage caused by an employee collaborating with criminal organizations, and damage to critical IT systems resulting from a natural disaster. All of these scenarios were found to pose a high level of risk. The study recommends the implementation of multi-factor authentication to prevent unauthorized access to port information systems, the provision of regular cybersecurity training for employees to raise awareness, the reinforcement of network security policies, and the enhancement of backup systems to ensure resilience against natural disasters.
[16]	Cyber Risk Management in Autonomous Passenger Ships	The study conducted a systematic literature review to identify cyber threats and classify risk factors for autonomous passenger ships. The findings indicate that the most significant threats in such vessels are associated with remote access vulnerabilities and weak network security. It was found that the Defense-in-Depth strategy alone is insufficient to mitigate complex cyberattacks. Accordingly, a new cybersecurity model was developed by combining the Defense-in-Depth approach with a Threat-Informed Defense strategy. The results further show that traditional security measures are inadequate for autonomous passenger ship systems due to the use of non-IP-based communication protocols. VPN tunnels are recommended to enhance cybersecurity in these systems

Cybersecurity and cyber risks in maritime transportation have become increasingly critical due to the rising levels of digitalization and automation. Recent academic research has primarily focused on port security, autonomous ships, various cyber threats, and risk management strategies. Studies in this field aim to understand the scope of cyber risks, identify potential threats, and develop mitigation strategies. Cybersecurity risks in the maritime industry can also be assessed through techniques such as bibliometric analysis and systematic literature reviews, which have been utilized in the existing literature (Table 2). While some of the studies in Table 2 analyze cyberattacks targeting autonomous ships and their consequences [19,20], others focus on cybersecurity management in port facilities [21]. Additionally, some studies propose solutions for addressing vulnerabilities in critical systems within the maritime sector [22,23].

Table 2 Bibliometric studies conducted in the relevant field

Author(s)	Domain	Purpose and Methods	Key Findings
[24]	Cyber Risk	This study examines cyber risk perception in the maritime sector using psychological models and systematically analyzes existing research. The study employs Okoli and Schabram's eight-step systematic literature review method, and 25 articles have been reviewed.	As a result of the analyses conducted in the study, 24 dimensions related to cyber risk perception were identified. Nine fundamental dimensions based on the psychometric paradigm—voluntariness, the immediacy of risk consequences, level of knowledge, controllability, catastrophic potential, dread, prevalence, novelty, and severity of consequences—were discussed in the maritime context alongside perceived benefits and optimism biases.
[20]	Cyberattacks	This study analyzes the types of cyberattacks on autonomous ships, their consequences, and existing security vulnerabilities. In this context, a comprehensive literature review was conducted using the PRISMA methodology to evaluate the industry's approaches to addressing these threats and identify its shortcomings.	The analyses indicate that autonomous ships' security systems can be easily breached, leading to significant financial losses, cargo loss, and disruptions in maritime traffic. Consequently, the findings highlight the need for stronger security measures in the industry. It has been concluded that defenses must be updated to counter next-generation attack techniques. To achieve this, the study emphasizes the necessity of adopting security-by-design approaches, implementing blockchain technologies, and enhancing international cooperation.
[21]	Cyber Security Risk Management	This study aims to systematically review the existing literature on cybersecurity risk management in port facilities, identify research gaps in this field, and provide guidance for future studies. In this context, a systematic literature analysis was conducted using studies retrieved from databases such as IEEE Xplore, ScienceDirect, and Scopus.	As a result of the analyses conducted, various models and recommendations have been proposed for port cybersecurity risk management. An Independent Maritime Cyber Assessment Organization has been suggested, and an Integrated Cyber Risk Assessment Model has been developed for port operations. The key challenges identified in this context include the heterogeneity of port environments, the management of cyber-physical dynamics, and the complexities involved in establishing standardized frameworks.
[23]	Cyber Security	This study aims to identify the challenges related to maritime cybersecurity, analyze existing solutions, and develop POSEIDON, a cybersecurity management framework designed to address these challenges. Accordingly, scientific studies were selected based on their focus on maritime cybersecurity. The analyses were conducted using bibliometric methods and content analysis.	The analysis results identified widespread security vulnerabilities in critical systems within the maritime sector, such as the AIS and the Electronic Chart Display and Information System (ECDIS). Furthermore, the study highlights the lack of an international standard and the challenges of protecting maritime infrastructure against cyber threats. The POSEIDON framework developed in this study integrates existing standards while introducing new elements that enhance security culture and automation systems.

Author(s)	Domain	Purpose and Methods	Key Findings
[22]	Cyber-Attacks	This study aims to examine scientific publications on cyber-attacks in the maritime sector and their impacts on shipboard sensors and systems using the bibliometric analysis method. In this context, 41 articles obtained from databases such as Web of Science were systematically reviewed. VOSviewer software was utilized for the analyses.	The analysis results indicate that cyber-attacks targeting sensors and systems in the maritime sector pose significant risks to global supply chain security, sustainability, and maritime safety. It has been found that with the increasing prevalence of automation systems, cyber-attacks have become more frequent while existing risk management methods remain insufficient. The study emphasizes the need to protect critical systems such as the Electronic Chart Display and Information System (ECDIS). Additionally, it has been determined that scientific publications in this field are predominantly produced by a specific group of countries and authors, with the United States, Brazil, Norway, Japan, and Croatia emerging as key contributors.
[25]	Risk and Reliability	This study aims to examine scientific publications on the security and reliability analysis of Maritime Autonomous Surface Ships published between 2015 and 2022 using bibliometric analysis while conducting a comprehensive literature review on these technologies' reliable design and risk assessment. Accordingly, a literature sample comprising 118 articles selected from Web of Science, Scopus, and Google Scholar was subjected to bibliometric analysis.	As a result of the bibliometric analysis, it has been determined that topics such as collision avoidance, software failures, hazard assessment, and human-machine interaction have received significant attention. The findings indicate a lack of dynamic approaches in risk assessment methods, the need for a more comprehensive examination of human-machine collaboration, and the limited number of studies in the literature focused on enhancing the reliability of communication systems.
[26]	Cyber Threat and Cyber Risk	This study aims to examine threat modeling and risk assessment methods in the maritime sector and identify the strengths and weaknesses of cybersecurity applications in ships. Through a systematic literature review, the study seeks to develop standardized frameworks for risk management in autonomous ships. The analysis covers various ship systems, including ship networks, navigation systems, cargo management systems, and engine control systems. A total of 25 articles published between 2015 and 2023 were analyzed, utilizing data from IEEE Xplore, Scopus, Web of Science, ACM Digital Library, and ScienceDirect.	The results of the analysis indicate that methods such as MaCRA, FMEA/FMECA, and STPA effectively assess risks specific to ship operations. It has been determined that attack tree modeling facilitates the identification of vulnerabilities and potential threat pathways in ship systems, while Bayesian Networks significantly contribute to modeling uncertainties and enhancing decision-making processes.
[27]	Cyber Security	This study aims to systematically review research conducted in maritime cybersecurity between 2013 and 2023, analyzing the ten-year development in this domain. The data used in the study were obtained from databases such as Google Scholar, Scopus, and ACM. Accordingly, 319 articles published between 2013 and 2023 were analyzed.	The study's findings indicate that interest in maritime cybersecurity significantly increased between 2016 and 2020. In recent years, more in-depth experimental studies and articles proposing solutions have been published on this topic. The research reveals that maritime cybersecurity studies are categorized into various subtopics, including port security, ship security, autonomous vessels, human factors, policy, and legal regulations. Moreover, studies in this field highlight cyber-attacks targeting critical systems such as the Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS), and Voyage Data Recorder (VDR).

Author(s)	Domain	Purpose and Methods	Key Findings
[19]	Cyber Risk, Safety & Reliability	This study uses bibliometric analysis to examine scientific publications on the risk, safety, and reliability analysis of autonomous ships in the maritime domain. The analysis aims to establish regulatory frameworks to enhance the safety of autonomous ships and identify research trends and gaps in this field. In this context, 417 articles published between 2011 and 2022 were analyzed using the R programming language and the Bibliometrix Shiny application based on data from the Scopus and Web of Science databases.	The analysis results of the study indicate that significant research efforts have been concentrated on navigation safety and collision avoidance. Among the reviewed publications, methods such as System-Theoretic Process Analysis and Bayesian Networks are the most frequently employed approaches. The study further reveals that China, Norway, and the United States are among the most productive countries in this field, establishing strong collaboration networks among themselves. Additionally, European and North American countries have been identified as having substantial potential for collaboration in this area. According to the reviewed studies, research gaps in this field include software failures, hardware malfunctions, human-machine interactions, and online risk monitoring systems.
[28]	Cyber Security	This study aims to analyze scientific publications in maritime cybersecurity to identify research trends and potential research areas in this domain. Within this scope, a literature search was conducted in the Scopus database, and studies published between 2013 and 2023 were analyzed using the VOSviewer software. These analyses provided a detailed classification of cyber-attack vectors in ships, ports, and the maritime logistics sector.	Among the attack methods identified in the study are signal jamming, data manipulation, information eavesdropping, and denial-of-service (DoS) attacks. The analysis results indicate that, in the context of maritime cybersecurity threats, the manipulation of GPS and AIS signals, false collision warnings, and system failures are prominent concerns. To mitigate these risks, the study emphasizes the need for cybersecurity training, awareness programs, and the enforcement of international regulations. Furthermore, the findings reveal that most scientific research models in this field are based on theoretical foundations, with a notable lack of practical applications.

Research in this field has primarily focused on identifying risks across various subdomains, assessing existing threats, discussing necessary countermeasures, and enhancing security measures and system reliability. Studies highlight vulnerabilities in critical maritime systems such as the Automatic Identification System (AIS), the Electronic Chart Display and Information System (ECDIS), and the Voyage Data Recorder (VDR). To address these challenges, it has been suggested that a comprehensive examination of human-machine interactions is necessary [25] and that developing international standards and legal regulations in this domain is essential [23]. It is believed that testing theoretical models through real-world applications and implementing digital technologies such as blockchain [20] could play a significant role in mitigating existing security vulnerabilities. A bibliometric review of studies employing bibliometric methods in this field has revealed that cybersecurity research in maritime transportation can be categorized into three main areas: cybersecurity and risk management in autonomous ships, cybersecurity in port and maritime infrastructure, and types of cyber-attacks and threats in the maritime sector.

Although autonomous ships significantly transform the maritime transportation industry, they remain highly vulnerable to cyber threats. The study conducted by [20] highlights that the security systems of autonomous ships can be easily breached, leading to financial losses, cargo disruptions, and interruptions in maritime traffic. Similarly, [25] emphasizes the necessity of reviewing security protocols used in Maritime Autonomous Surface Ships (MASS), focusing on risk and reliability assessments. [19] conducted a bibliometric review on risk, safety, and reliability in autonomous ships, revealing significant research gaps in the literature regarding software failures, human-machine interactions, and collision avoidance systems. On the other hand, [26] provides a detailed examination of threat modeling and risk assessment methods in maritime cybersecurity, analyzing existing strategies' strengths and weaknesses. Their study comprehensively evaluates current cybersecurity approaches, highlighting areas that require further improvement and adaptation to evolving cyber threats in the maritime sector.

Cyber-attacks in the maritime sector are primarily targeted at ship networks, sensor systems, and electronic chart systems. [22] conducted a bibliometric analysis revealing that cyber-attacks on maritime sensors and systems pose significant risks to global supply chain security and maritime safety. Their study high-

lights that the increasing prevalence of automation systems has increased cyber threats while existing risk management methods remain inadequate. Similarly, [28], in a comprehensive literature review on maritime cybersecurity, categorized attack vectors in ship and port systems, emphasizing that the primary cyber risks include GPS and AIS signal manipulation, false collision warnings, and system failures. Studies analyzing general research trends in maritime cybersecurity aim to identify gaps in the existing literature and guide future research. [24] investigate cyber risk perception in the maritime sector using psychological models, assessing how individuals perceive cyber risks. [27] conduct a ten-year analysis of maritime cybersecurity research, revealing that research trends accelerated significantly between 2016 and 2020. Their study highlights key developments and emerging areas of focus in maritime cybersecurity, providing valuable insights for future studies. The research highlights that maritime cybersecurity encompasses various subdomains, including port security, autonomous ships, human factors, and legal regulations, emphasizing the need for more empirical studies. [28] Point out that most models in the literature are based on theoretical foundations, while practical applications remain insufficient. Their study underscores the necessity of bridging the gap between theory and real-world implementation to enhance the effectiveness of cybersecurity strategies in the maritime sector.

Cybersecurity research in the maritime sector exhibits several commonalities. Many studies emphasize the vulnerability of critical maritime systems to cyber-attacks and highlight the need to strengthen security measures through international collaboration [20,23]. Similarly, some studies adopt a narrower focus, offering more specific assessments on particular topics within maritime cybersecurity, such as risk management in autonomous ships, cyber threats in port infrastructure, and security protocols for navigation systems. These focused evaluations contribute to a more detailed understanding of specific challenges while reinforcing the broader need for comprehensive cybersecurity strategies in the maritime industry. For instance, [20] and [25] focus on cyber-attacks targeting autonomous ships, analyzing their vulnerabilities and potential countermeasures. In contrast, [21] concentrates on cybersecurity management in port facilities, emphasizing the need for integrated risk assessment models. Meanwhile, [22] and [28] take a direct approach to maritime cyber threats, examining attack vectors in detail and providing insights into how cyber-attacks are executed within the maritime sector. These studies collectively contribute to a comprehensive understanding of maritime cybersecurity by addressing various threats, vulnerabilities, and defense mechanisms.

One of the key differentiating aspects of these studies is the methodologies employed. For instance, [22] uses VOSviewer to conduct bibliometric analysis, whereas [24] adopts a systematic literature review approach. Additionally, some studies focus on sector-specific policies and strategies [23], emphasizing regulatory frameworks and international cooperation, while others adopt more technical approaches, proposing risk assessment models tailored to maritime cybersecurity [26]. This diversity in methodologies highlights the multidimensional nature of maritime cybersecurity research, encompassing policy-driven, theoretical, and technical perspectives. In conclusion, addressing security vulnerabilities in the maritime sector requires technical solutions and consideration of regulatory and operational dimensions. Additionally, further empirical research is needed to explore how next-generation security solutions, such as blockchain, can be effectively implemented in the industry. While significant progress has been made in maritime cybersecurity research, developing more effective strategies to counter existing threats necessitates increased interdisciplinary studies. In particular, proposed security frameworks must be supported by field studies to ensure their practical applicability and effectiveness in mitigating cyber risks in real-world maritime operations.

3 Method, analysis, and findings

To ensure the cumulative advancement of scientific knowledge, systematically synthesizing research findings and data available in the literature is essential. In this regard, bibliometric analysis is a quantitative and objective method for examining scientific literature within a particular discipline [29(p. 166)]. This method enables the assessment of the scope and growth trends of literature in a given field, providing insights into potential contributions to future research [30 (p. 1004)]. Citation counts, publication volumes, and keywords are frequently used in large-scale and highly objective data types in bibliometric analysis. This analytical method is crucial in structuring and making sense of unstructured data, transforming it into organized and meaningful insights. As a result, bibliometric analysis helps decode a research field's development trajectory and enhances comprehension through visualization techniques [31]. Consequently, the comprehensive data derived from scientific research allows for an in-depth examination of the evolution of cumulative knowledge over time, thereby establishing a robust foundation for future studies in the respective field [32 (pp. 1014–1015)]. In recent years, accessing large-scale datasets in databases such as Scopus and Web of Science have become increasingly convenient. Additionally, the use of open-source bibliometric software has become more widespread, making this method a preferred choice for analyzing scientific studies across various disciplines [33,34].

Different software tools with various functionalities are utilized to assess scientific productivity in a given field and analyze its intellectual structure. Gephi, VOS-

viewer, and CiteSpace are commonly used for visualization purposes. Furthermore, Bibliometrix, compatible with the R programming language, stands out due to its ability to perform multi-faceted analyses, including source impact assessment, document analysis, keyword analysis, and data visualization [35 (pp. 156–158)].

In this context, the R programming language was chosen to conduct the analyses in this study. The analysis stages are illustrated in Figure 1. As part of the bibliometric analysis, a search was conducted in the Web of Science database using the keywords "maritime" OR "shipping" OR "seafaring" OR "maritime industry" OR "marine industry" OR "maritime supply chain" in conjunction with "cybersecurity" OR "cyber risk" OR "cyber threats" OR "cyber risk management." As a result, the total number of publications retrieved was determined to be 252. Subsequently, a language restriction was applied, and only publications written in English were included in the analysis, reducing the total number of publications to 248. Given the limited number of studies in this field, all publication categories indexed in the Web of Science, including Conference Proceedings Citation Index (CPCI-S) and Book Citation Index – Social Sciences & Humanities (BKCI-SSH), as well as SSCI,

Figure 1 Data collection and analysis stages

SCI-Expanded, AHCI, and ESCI, were selected for inclusion in the study. The study examined various data regarding the citation counts of 248 publications over the years and their distribution. The keywords used in the articles were analyzed through factor analysis, and trends related to these keywords were investigated. Accordingly, the proximity and distance of the keywords used in the 248 publications were clustered through factor analysis, leading to the development of a conceptual structure map. The number of references cited by the publications and the distribution of citations received by these publications within the Web of Science (WoS) database were determined. Additionally, categorical clustering analyses were conducted, and findings related to authors, research domains, publication sources, and countries were presented through visual maps and tables generated using the R programming language.

In this study on cybersecurity applications in the maritime sector, 248 publications indexed in the Web of Science (WoS) database and published between 2014 and December 2024, including early access publications slated for 2025, were included in the analysis. These 248 publications were published across 136 different journals. The average number of citations per publication was 9.4, while the average number of co-authors per publication was 3.63. Among the years 2014–2025,

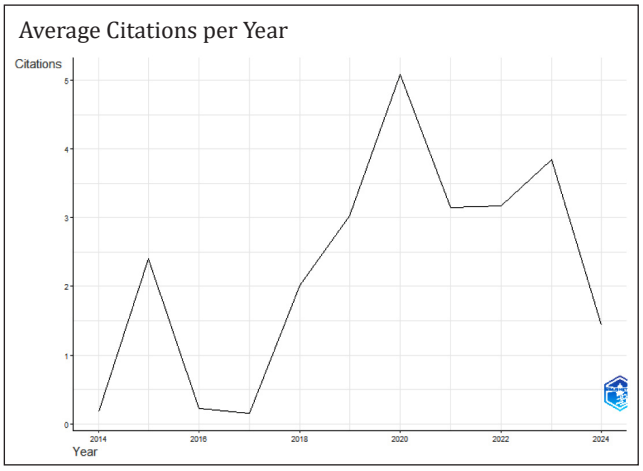

Figure 2 Citation counts and general characteristics by year

the highest average annual citation count was recorded in 2020 (Figure 2 and Table 3). The "MeanTCp" column in Table 2 represents the average number of citations per year. In 2020, 20 publications were produced on this topic, receiving an average of 5.08 citations per publication. This finding suggests that 2020 had a relatively high impact level compared to other years.

According to Table 3, 248 publications were evaluated for the period 2014–December 2024, including early

Table 3 General characteristics of the analyzed publications

Timespan	**2014-2025**	
Publication	248	
Journals	136	
Keywords	801	
Average Citations per Publication	9,411	
Number of Single-Authored Publications	33	
Average Number of Co-Authors per Publication	3.63	
International co-authorships %	27.82	
Year	**Number of Articles**	**Mean TC Per Year***
2014	2	0.18
2015	1	2.40
2016	1	0.22
2017	5	0.15
2018	19	2.02
2019	16	3.03
2020	20	5.08
2021	34	3.15
2022	42	3.17
2023	40	3.85
2024	66	1.44
2025	2	0.18

* Mean TC Per Year: Average Citations per Year

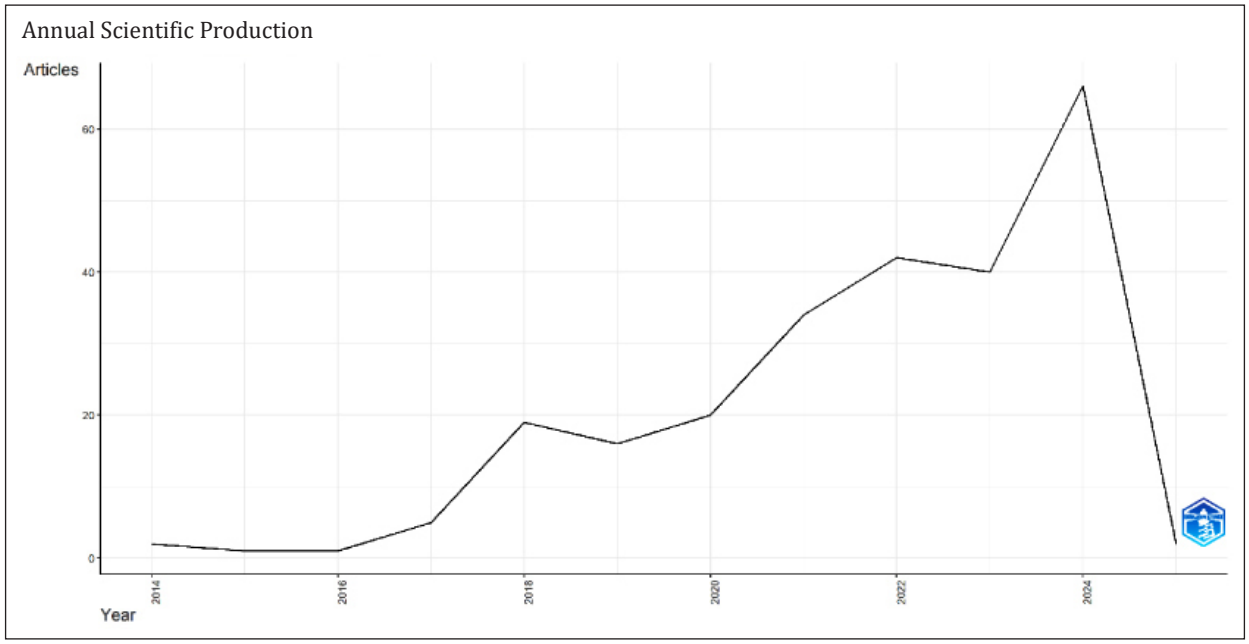

Figure 3 Annual scientific production

access publications slated for 2025. These publications were disseminated across 136 different journals. The average number of citations per publication was calculated as 9.41, highlighting the impact of the analyzed literature in the field and indicating that these studies have been frequently cited.

The analysis results reveal that the total number of single-authored publications is 33. Given the total number of publications (248), this finding suggests that a significant portion of the analyzed studies are collaborative in nature. The average number of co-authors per publication was also calculated as 3.63. Furthermore, the international collaboration index, measured at 27.82%, indicates a notable level of scientific collaboration in the literature within this research domain.

Upon examining the annual scientific production graph (Figure 3), it has been determined that publications in this field have shown a significant increase since 2018. Notably, during the 2023–2024 period, the number of publications in this domain has risen substantially, reaching its highest level. Among the analyzed years, 2024 is the most productive year, with 66 publications.

Keywords highlight the core themes of a publication, enhancing its academic visibility and facilitating more efficient and effective literature searches in relevant fields. This, in turn, improves the accessibility of publications and increases the efficiency of literature reviews on the subject.

In the word cloud presented in Figure 4, the size of each word varies based on its frequency of usage. Accordingly, the most frequently used keywords appear larger and are positioned closer to the center to enhance visual emphasis [36 (p. 74)].

The frequency table (Table 4) and word cloud (Figure 4) generated from the analysis illustrate the most frequently mentioned concepts and research trends in cybersecurity studies within the maritime sector. Accordingly, when analyzing the keywords of the 248 publications, it is observed that the most frequently used keyword is "framework." Following this, the second most frequently used keyword is "model," which is then followed by "security," "cybersecurity," "cyber security," "performance," "safety," "system," "design," "authentication," and "maritime," respectively.

The frequent usage of the terms "framework," "model," and "security" indicates that the literature on cybersecurity research in the maritime sector primarily focuses on defining theoretical frameworks and developing applicable models. The terms "cybersecurity" and "cyber security" appear in publications in two different forms, suggesting variations in their usage within the literature. Additionally, the prominence of the keywords "safety," "system," and "systems" highlights the emphasis on studies that underscore the importance of security in maritime operations.

The frequency of "design" and "authentication" in academic publications indicates a significant focus on system design and authentication processes in maritime cybersecurity applications. The findings suggest that the maritime sector stands out as a specific domain where cybersecurity applications are concentrated. The term "maritime" in the frequency table signifies that scientific studies in this field address sector-specific appli-

Table 4 Most frequently used keywords

Terms	Frequency
framework	18
model	18
security	18
cybersecurity	17
cyber security	9
safety	7
system	7
systems	7
design	6
authentication	5
maritime	5

Figure 4 Word cloud

cations, threats, and solutions. However, the relatively low frequency of this term may indicate that niche areas, such as cybersecurity in the maritime sector, are discussed less frequently in the literature.

Figure 5 illustrates the evolution and changes in prominent terms within the literature on cybersecurity applications in the maritime sector over the years. This graph provides insight into the areas that have increased focus in the literature over time.

Accordingly, the terms "framework" and "model" have been extensively used, particularly in 2024. This suggests a growing interest in theoretical frameworks and modeling studies within the maritime cybersecurity literature. The term "security" has consistently increased since the initial studies in this field, and according to the current dataset, its highest frequency is observed in the year 2025. Similarly, the term "cybersecurity" follows a comparable trend, indicating a sustained rise in research interest in this area. However, as we are still in early 2025, this observation should be interpreted with caution, as the data may not yet fully reflect the year's publication trends. This indicates that

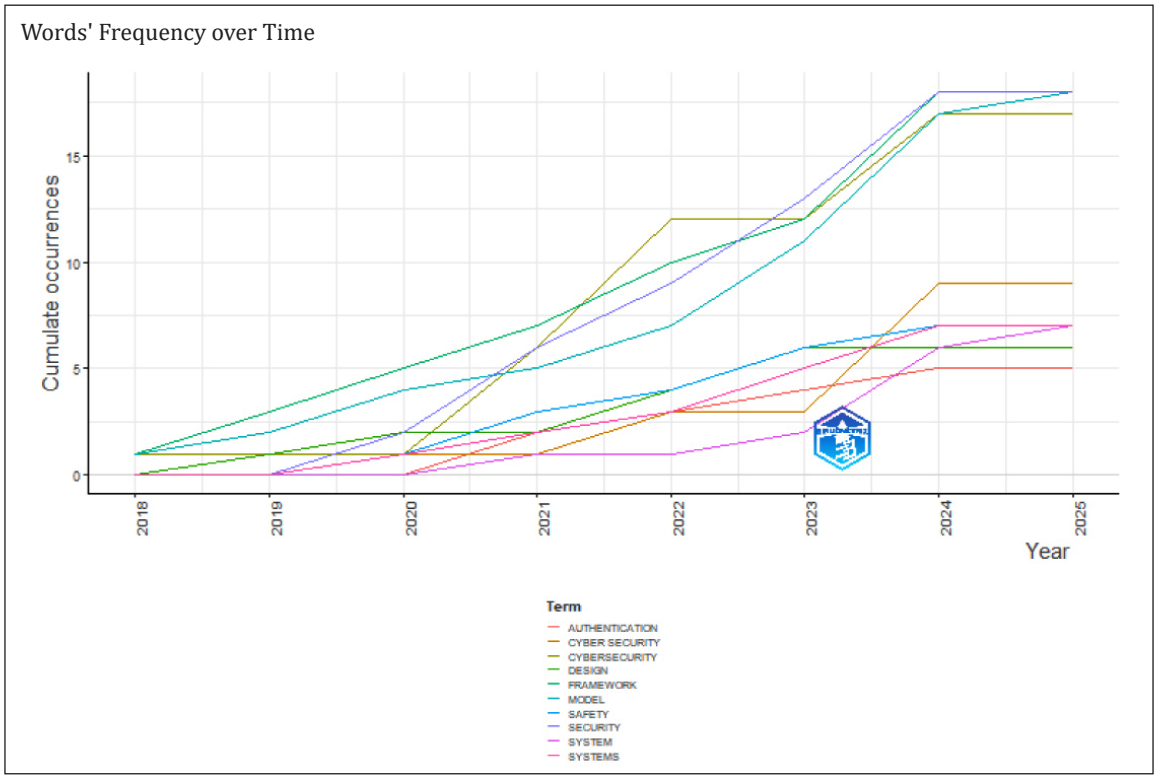

Figure 5 Keyword trends

cybersecurity will remain a significant theme in maritime sector research. Most of the terms identified in the analysis have shown a noticeable upward trend since 2020. This increase can be associated with the acceleration of Industry 4.0 technologies in the maritime sector and the growing focus on cybersecurity due to increasing digitalization processes [37–39].

Figure 6 visualizes the key themes in cybersecurity research within the maritime sector, their levels of development, and the centrality of their relationships with other themes. The map reveals that the themes are divided into four distinct regions.

The themes "framework model" and "collision-avoidance navigation" exhibit high centrality and density, indicating that these topics are prominent in maritime cybersecurity research and are extensively addressed in scientific studies. The "framework model" is a focal point for developing theoretical frameworks and practical applications in maritime cybersecurity. Its prominence underscores the importance of establishing comprehensive solutions in cybersecurity applications. Similarly, "collision-avoidance navigation" emerges as a critical subtheme in ensuring safe navigation for autonomous maritime vehicles. Collisions in the maritime sector are among the most severe accidents, necessitating the development of advanced collision-avoidance systems, particularly for autonomous ships. Factors such as collision prevention [40], the development of autonomous navigation [41], minimizing human errors [42], compliance with regulations and the integration of advanced artificial intelligence systems [43], and enhancing data collection and processing capabilities [44] further emphasize the significance of this topic.

In Figure 6, themes such as "ships performance" and "automation" exhibit high density but low centrality. This suggests that while highly specialized researchers explore these themes, their overall influence remains limited.

These findings indicate that research in these areas is conducted with a narrower academic focus. However, despite their limited reach, such studies are crucial in offering solutions to specific problems within maritime cybersecurity.

Themes such as "security cybersecurity," "system internet," and "models risk" in Figure 6 exhibit high centrality but low density. This indicates that these topics are strongly connected to other themes in the field but have not yet been extensively explored in the academic literature.

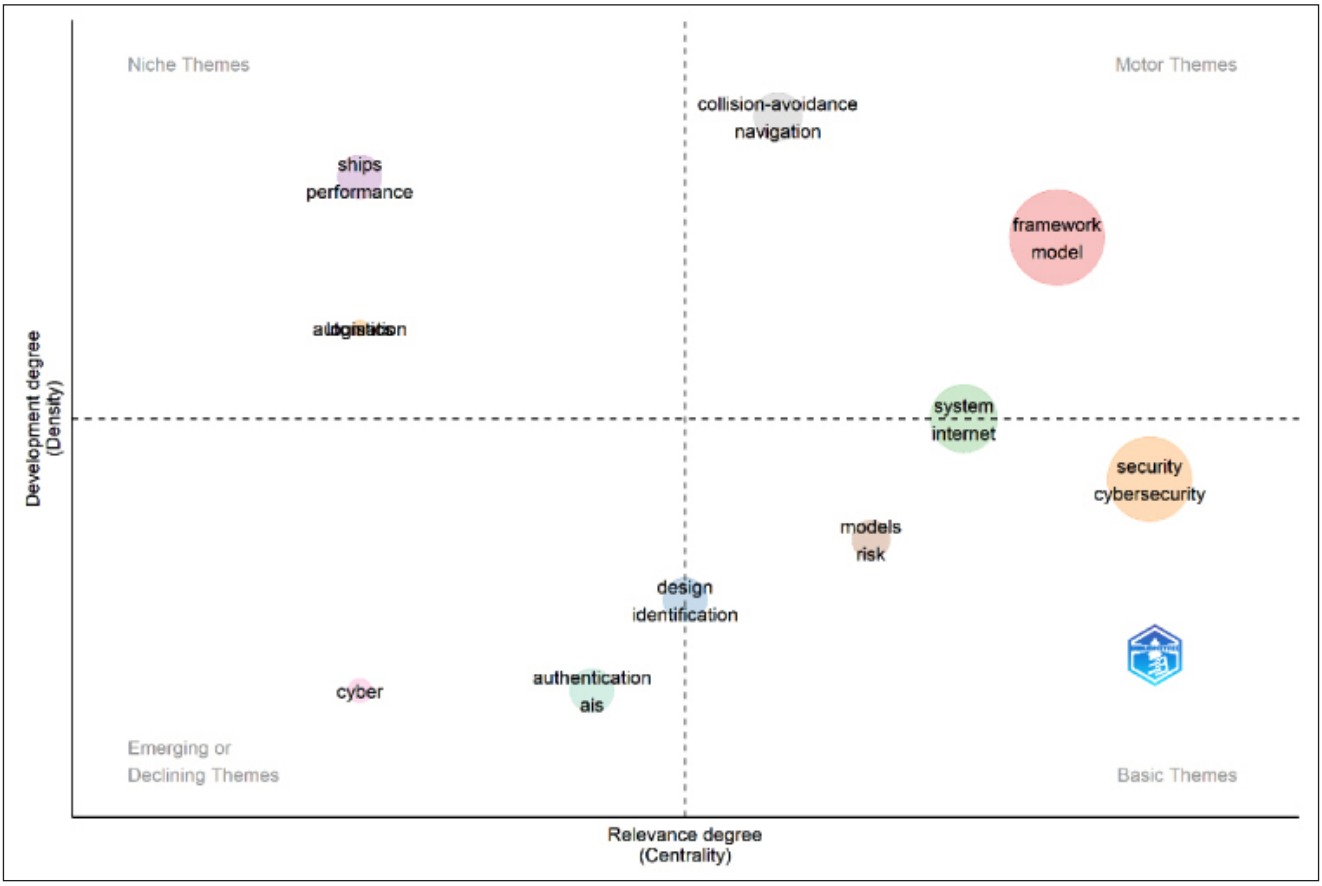

Figure 6 Thematic distribution in maritime and cybersecurity literature: density and centrality analysis

Table 5 Sources impact

Source	h_index	TC*	NP**	PY_start
Journal of Marine Science and Engineering	7	173	16	2019
TRANSNAV – International Journal on Marine Navigation and Safety of Sea Transportation	6	141	15	2018
Journal Of Navigation	5	116	6	2018
Sensors	5	55	7	2021
WMU Journal of Maritime Affairs	4	118	6	2019
2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CYBER SA)	3	26	3	2019
Computers & Security	3	53	4	2021
IEEE Access	3	45	5	2020
Journal of Information Security and Applications	3	37	3	2021
Journal of Transportation Security	3	42	3	2018
Marine Technology Society Journal	3	23	3	2018
Proceedings Of The 2021 IEEE International Conference on Cyber Security and Resilience (IEEE CSR)	3	29	4	2021
Safety Science	3	119	3	2020
Transactions on Maritime Science-TOMS	3	41	7	2019
2022 IEEE International Conference on Cyber Security and Resilience (IEEE CSR)	2	17	5	2022
Applied Sciences-Basel	2	73	4	2020
Asian Journal of Shipping and Logistics	2	33	2	2021
Computer Security, ESORICS 2019	2	9	2	2020
Information	2	58	2	2022
International Journal of Critical Infrastructure Protection	2	46	4	2021

* TC: Total number of citations, **NP: Total number of publications.

On the other hand, "cyber" and "authentication AIS" are characterized by both low centrality and low density. These findings suggest that these topics are still being developed in maritime cybersecurity research. As a result, these areas present potential opportunities for researchers looking to conduct innovative studies in this domain.

Table 5 presents the key journals in which 248 publications related to cybersecurity applications in the maritime sector have been published. Among them, the Journal of Marine Science and Engineering stands out as the journal with the highest number of publications (16) and the most citations in this field between 2014 and 2024.

The TransNav – International Journal on Marine Navigation and *Safety of Sea Transportation* ranks second in terms of both the number of publications and citations, positioning itself as an influential journal for cybersecurity research in the maritime sector.

The H-index measures a journal's productivity and citation impact. In this study, the *Journal of Marine Science and Engineering, TransNav – International Journal on Marine Navigation* and *Safety of Sea, Journal of Navigation*, and *Sensors* have the highest H-index among the analyzed journals. These findings indicate that studies published in these journals are frequently cited in the academic literature on maritime cybersecurity, highlighting their significance and impact in the field.

Local citations refer to the number of times an author within a given dataset is cited by other publications within the same dataset. The findings obtained in this context allow for both the evaluation of overall citation impact and a deeper examination of the connections between documents within the dataset [45 (p. 5)]. Table 6

Table 6 Most locally cited authors

Author	Local Citations
Svilicic Boris	65
Tam Kimberly	63
Jones Kevin	53
Brosset David	42
Androjna Andrej	37
Pavic Ivica	35
Gkioulos Vasileios	34
Bernsmed Karin	32
Meland Per Håkon	32
Nesheim Dag Atle	32
Andonovic Ivan	29

Table 7 Author production over time

Author	Publication years	freq	TC*	TCpY**
Amro Ahmed	2020-2022-2023-2024	8	54	21.733
Bolat Pelin	2019-2021-2022-2023-2024	9	56	21.083
Bolbot Victor	2020-2022-2023-2024	7	147	**57.067**
Gkioulos Vasileios	2020-2021-2022-2023-2024	**14**	108	41.383
Jones Kevin	2018-2019-2024	5	101	18.024
Katsikas Sokratis	2020-2021-2022-2023-2024	7	79	22.917
Kayisoglu Gizem	2019-2021-2022-2023-2024	9	56	21.083
Oruc Aybars	2022-2024	7	36	16.000
Svilicic Boris	2018-2019-2020	7	**154**	26.171
Tam Kimberly	2018-2019-2022-2023-2024	13	131	34.191

* TC: Total number of citations, ** TCpY: Total citations per year

presents the authors with the most local citations in this context. According to the findings, Boris Svilicic is the most locally cited author, receiving 65 citations. Following him, Kimberly Tam and Kevin Jones rank second and third, with 63 and 53 citations, respectively.

These results indicate that the publications by these authors stand out within the dataset analyzed in this study and are frequently used as key references in maritime cybersecurity research.

Table 7 presents the top 10 most prolific authors in maritime cybersecurity research, detailing their active publication years, publication frequency (freq), total citation count (TC), and annual average citation impact (TCpY). The data compiled in Table 7 aims to evaluate the authors' contributions to the literature quantitatively and qualitatively.

Among the top 10 most publishing authors, Gkioulos Vasileios stands out as the most productive researcher in this field. Between 2020 and 2024, he consistently published in journals indexed in the Web of Science database, producing 14 publications. Victor Bolbot has seven publications and has received an average of 57.067 citations per year (TCpY). This indicates that his studies in this field have greatly impacted maritime cybersecurity research. Meanwhile, Boris Svilicic is the most cited author, receiving 154 citations (TC) from his seven publications between 2018 and 2020. This highlights his significant influence in the academic literature on maritime cybersecurity.

Table 8 presents the countries with the highest number of publications in cybersecurity in maritime studies. According to the data, the top five countries in this area are as follows: Norway (91 publications), the United Kingdom (83 publications), the United States (69 publications), Greece (47 publications), China (37 publications), and Finland (37 publications). The primary reasons for the high scientific productivity in Norway and the United Kingdom include the significant role of the maritime sector in their economies and the concentration of research in maritime technologies. In particular, Norway experienced over 50 cyberattacks in the energy, oil, and gas sectors in 2015 [46]. With the advancement of digital technologies, cybercrime threats have increased, prompting the Norwegian Maritime Industry to establish the Norwegian Maritime Cyber Resilience Centre in 2021 [47]. The United Kingdom, one of the leading maritime nations in the world, developed a new maritime security strategy in 2022, targeting the latest physical and cyber threats with a five-year plan [48]. In 2022, the United States implemented the Strengthening American Cybersecurity Act of 2022 [49]. This law established various action plans to foster international cooperation in cybersecurity. Implementing these actions will elevate global maritime cybersecurity standards [50]. The Chinese government, aware of the cybersecurity risks in maritime operations, established the National Cybersecurity Center campus in 2017 to address critical security vulnerabilities in key sectors, including maritime operations, and strengthen cybersecurity [51]. In the same year, China enacted the Cybersecurity Law of the People's

Table 8 Countries with the highest number of publications

Country	Freq
Norway	91
UK	83
USA	69
Greece	47
China	37
Finland	37
South Korea	25
Croatia	22
France	22
Spain	21
Cyprus	19
Germany	19

Republic of China [52]. Furthermore, it is projected that by 2025, the cybersecurity market size in the United States will reach 88 billion USD [53], while in China, it is expected to reach 16 billion USD [54], indicating that cybersecurity represents a significant market for these countries. Based on this data, the prominence of leading universities and research centers in these countries in terms of the number of scientific studies on maritime cybersecurity clearly demonstrates the importance given to cybersecurity research.

Figure 7 represents the collaboration network of authors in maritime cybersecurity studies. Each node in the network represents a researcher, while the lines connecting the nodes indicate collaborative efforts between these individuals. The nodes' size reflects the authors' centrality within the network or the intensity of their collaborations. The colors represent different collaboration clusters. The collaboration network among the authors consists of multiple distinct clusters. This situation suggests that maritime cybersecurity research focuses on various sub-disciplines, with these sub-disciplines forming collaborations within themselves. This indicates that knowledge sharing and interdisciplinary collaborations within the literature are limited. As a result, the connections between the clusters are relatively weak. In the figure, Gkioulos Vasileios and Tam Kimberly stand out as the two prominent leaders of the network.

Table 9 evaluates maritime cybersecurity studies based on each country's total citation count (TC) and average article citation indicators. According to the data, the United Kingdom has the highest total citation count (427), highlighting the country's leadership in maritime cybersecurity research. Although Norway has a lower average citation value than the United Kingdom, it ranks second in total citations (349). Conversely, Spain leads in terms of the highest average citation performance (33.4) for studies in this field. This result indicates that Spain has published fewer studies than the United Kingdom, Norway, Croatia, and the United States, but these studies have had a higher impact. Similarly, while having a lower total citation count compared to these countries (65), Qatar stands out as a country with high-impact publications in the field due to its high average citation performance (32.5).

Table 9 Countries with the most citations

Country	TC*	Average Article Citations
United Kingdom	427	15.8
Norway	349	10.9
Croatia	176	19.6
USA	176	7.0
Spain	167	33.4
Korea	124	17.7
Greece	91	6.5
Finland	85	7.7
Slovenia	82	27.3
Qatar	65	32.5
Denmark	64	16.0
Germany	51	8.5
France	47	7.8
Netherlands	43	43.0
Turkey	42	14.0

* TC: Total number of citations

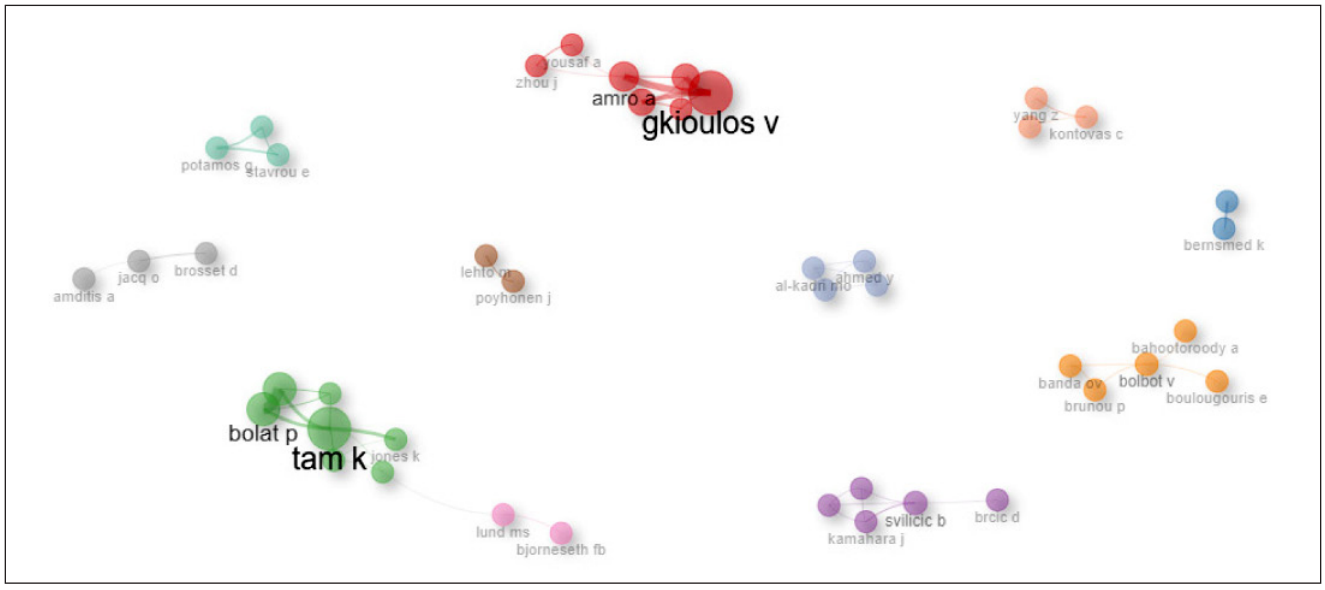

Figure 7 Academic collaboration among authors

Table 10 represents the scientific collaboration network among countries in maritime cybersecurity studies. The data in the table numerically expresses the collaborations between countries, while the global collaboration map shows the geographical distribution of these data. According to Table 10, the countries with the most collaborations in this field are the United Kingdom and Greece (f: 5). Following these two countries, the following most collaborative countries are China and Finland (f: 4), Greece and France (f: 4), and Norway and the United Kingdom (f: 4). These results suggest that with the rapid advancement and spread of digital technologies across all sectors in recent years, international collaboration in maritime cybersecurity studies is also open to further development.

Table 10 Countries with the highest collaboration frequency

From	To	Frequency
United Kingdom	Greece	5
China	Finland	4
Greece	France	4
Norway	United Kingdom	4
Brazil	Portugal	3
Croatia	Japan	3
Croatia	Slovenia	3
Finland	Netherlands	3
Greece	Spain	3
Korea	Australia	3

Figure 8 visually represents the collaboration network among countries in maritime cybersecurity studies, geographically mapping the relationships. The lines on the map indicate collaboration between countries, while the intensity of the countries' colors reflects the frequency of these collaborations. The collaboration map shows that European countries and China are at the center of the collaboration networks, while the Asia-Pacific region and North America have less densely connected networks. The data suggest that these regions are open to efforts to increase international collaborations in the coming years. With the increase in scientific publications and international collaborations in this field, it is believed that more innovative and solution-oriented approaches can be developed to integrate cyber technologies into the global maritime system.

Figure 9 displays the total academic collaboration map for countries publishing on cybersecurity applications in maritime studies. This map represents the total number of collaborations between a country and others worldwide. The United States, China, and Northern and Western European countries are marked in dark blue, indicating that these countries engage in a higher level of academic collaboration overall. The results suggest that these countries play a global leadership role in maritime cybersecurity research. India, Australia, and South Korea are highlighted in light blue-green tones,

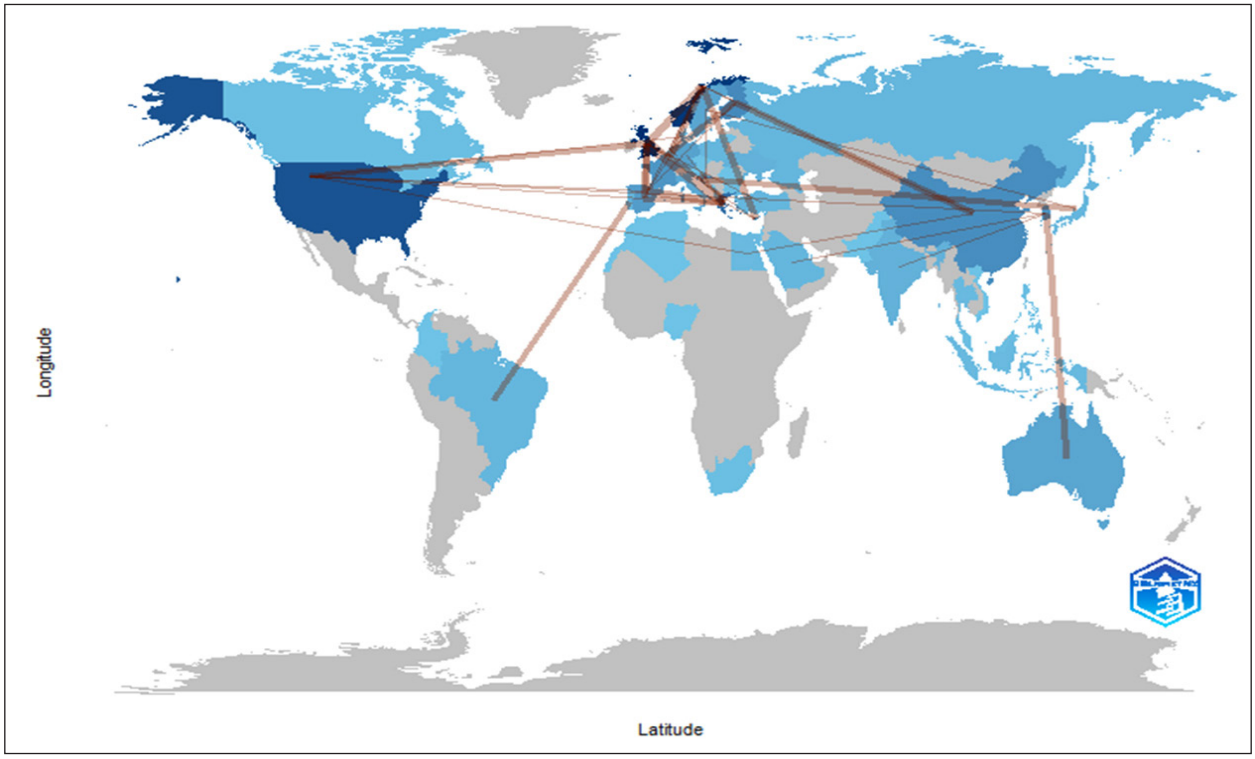

Figure 8 Countries' collaboration map

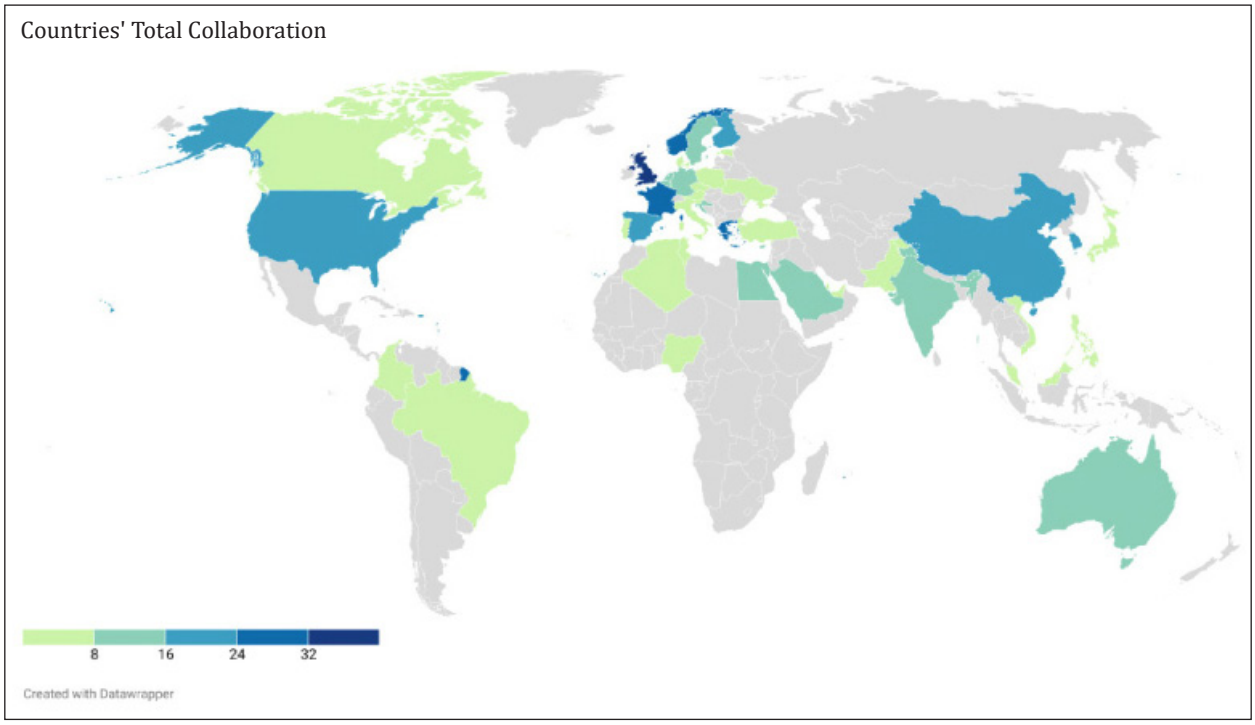

Figure 9 Countries' total collaboration map

representing countries with a medium level of collaboration. This indicates that while these countries are part of regional or international collaboration networks, they do not contribute as extensively to scientific research as the leading countries. South America, Africa, and some Asian countries are generally marked in light green tones. These findings suggest that the involvement of these countries in maritime cybersecurity research is limited. Developing countries, such as those in Africa, South America, and South Asia, exhibit low levels of collaboration in this field. This situation proves that cybersecurity issues in the maritime sector are not sufficiently prioritized in these regions, and there are limited resources, investments, and, consequently, scientific research in information and communication technologies. Along maritime trade routes, these countries are at a higher risk from cyber threats. Therefore, it can be argued that strengthening international funding and collaboration mechanisms is necessary to raise awareness of maritime cybersecurity and enhance research capacities in developing countries.

Figure 10 shows the distribution of corresponding authors by country in maritime cybersecurity studies and the level of collaboration between countries. The number of publications published by a country alone (SCP: Single Country Publications) or through collaboration with multiple countries (MCP: Multiple Country Publications) is shown comparatively on the graph. Norway, which ranks first in the distribution of corresponding authors by country, has produced most of its publications without collaborating with other countries. The United Kingdom, which ranks second in the distribution of corresponding authors by country, has placed greater emphasis on international collaboration than Norway. This indicates that the United Kingdom is open to global academic collaborations. The United States, which ranks third in the distribution of corresponding authors by country, has conducted a significant portion of its studies independently. This finding regarding the United States can be interpreted as reflecting the country's strong research infrastructure in digital technologies and security, with less focus on international collaborations compared to Norway and the United Kingdom.

Table 11 presents the university rankings based on publications in maritime cybersecurity studies. The university with the most publications in this field is the Norwegian University of Science and Technology in Norway, with 48 publications. Istanbul Technical University follows it in Turkey with 22 publications, and Plymouth University in the United Kingdom with 20 publications. Notably, the countries leading the ranking in terms of publication numbers are located in the European region. Rijeka University in Croatia, Aalto University and Jyväskylä University in Finland, and the University of the Aegean in Greece actively work in maritime and cybersecurity. This indicates that Europe plays a significant role in academic research in this area. Additionally, including the Wuhan University of Technology from China in this list suggests a global perspective in research on this topic.

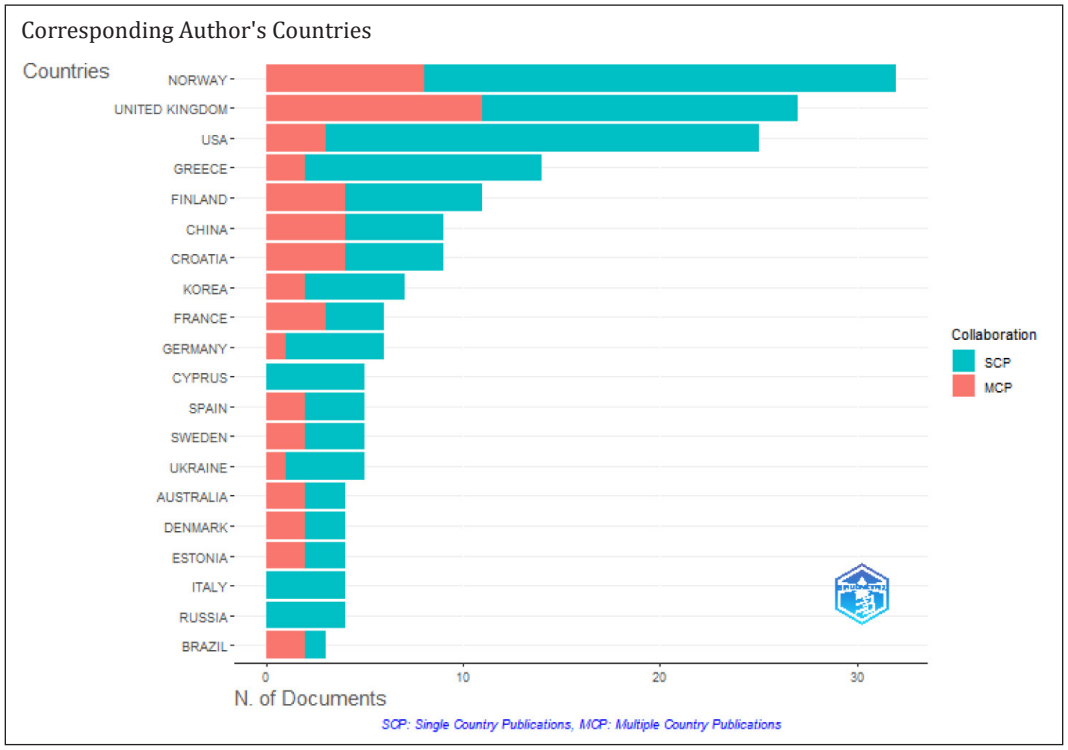

Figure 10 Distribution of corresponding authors by country and level of collaboration

Table 11 Universities based on publication numbers

Affiliation	Countries	Articles
Norwegian University of Science and Technology	Norway	48
İstanbul Technical University	Türkiye	22
University of Plymouth	United Kingdom	20
University of Rijeka	Croatia	18
Open University of Cyprus	Cyprus	15
Wuhan University of Technology	China	14
University of Piraeus	Greece	12
Aalto University	Finland	12
University of Jyväskylä	Finland	11
University of the Aegean	Greece	10

The most globally cited studies reveal that academic interest in maritime cybersecurity is shaped by themes such as digital transformation, cyber risk assessment, and autonomous maritime systems. The most highly cited work by [55], which focuses on Industry 4.0 applications in the maritime domain, underscores the fundamental role of digitalization in shaping cybersecurity research. Similarly, model-based risk assessment approaches developed by [56] and [11] demonstrate a strong scholarly interest in practical tools for evaluating cybersecurity risks in ship systems. In addition to methodological advancements, the works of [57] and [58] indicate an ongoing academic effort to synthesize knowledge and identify emerging threats, particularly in IoT and automation areas. Moreover, empirical assessments such as the study by [9], which investigates security vulnerabilities in ship systems, highlight the operational dimension of cyber risk and the critical importance of securing navigation technologies such as ECDIS. Similarly, the studies by [59] and [60] draw attention to vulnerabilities in AIS systems, while the works of [61] and [62] emphasize the need for secure and reliable solutions in autonomous vessel operations. Overall, the most cited publications reflect a multidisciplinary trend in maritime cybersecurity research, integrating technological, operational, and strategic perspectives that continue to guide the development of the field.

Table 12 The Most Global Cited Documents

Author(s)	Article Title	Source	TC*	TCpY**
[55]	Industry 4.0 in the port and maritime industry: A literature review	Journal of Industrial Information Integration	125	20.83
[56]	A novel cyber-risk assessment method for ship systems	Safety Science	67	11.17
[11]	MaCRA: a model-based framework for maritime cyber-risk assessment	WMU Journal of Maritime Affairs	66	9.43
[63]	Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis	Systems Engineering	50	8.33
[61]	Collaborative collision avoidance for Maritime Autonomous Surface Ships: A review	Ocean Engineering	48	12.00
[9]	Maritime Cyber Risk Management: An Experimental Ship Assessment	The Journal of Navigation	47	6.71
[57]	Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends	Information	46	11.50
[64]	Assessing Cyber Challenges of Maritime Navigation	Journal of Marine Science and Engineering	43	7.17
[58]	A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry	IEEE Transactions on Intelligent Transportation Systems	43	14.33
[62]	A multinomial process tree for reliability assessment of machinery in autonomous ships	Reliability Engineering & System Safety	43	8.60
[65]	Vessels Cybersecurity: Issues, Challenges, and the Road Ahead	IEEE Communications Magazine	41	6.83
[66]	A novel risk assessment process: Application to an autonomous inland waterways ship	Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability	40	13.33
[60]	A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System	TRANSNAV	38	4.75
[67]	Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue	Transport Policy	38	7.60
[68]	A Study on Identification of Development Status of MASS Technologies and Directions of Improvement	Applied Sciences	38	6.33
[69]	Enhancing Navigator Competence by Demonstrating Maritime Cyber Security	The Journal of Navigation	34	4.25
[59]	AIS Data Vulnerability Indicated by a Spoofing Case-Study	Applied Sciences	33	6.60
[17]	A Retrospective Analysis of Maritime Cyber Security Incidents	TRANSNAV	32	6.40
[70]	A BN driven FMEA approach to assess maritime cybersecurity risks	Ocean & Coastal Management	31	10.33
[15]	Cyber security risk assessment for seaports: A case study of a container port	Computers & Security	31	6.20

* TC: Total number of citations, ** TCpY: Total citations per year

4 Discussion and conclusions

The maritime sector is transforming significantly in response to increasing cybersecurity threats and risks driven by digitalization processes. In international maritime transportation, operators use cyber systems to transmit information about ships, cargo, and passengers. Digital technologies, including cyber systems, enhance the efficiency of operational processes in the maritime industry. However, these technologies also carry inherent risks. The misuse or disruption of cyber systems can lead to disruptions in the supply chain flow, interruptions in international trade, and significant economic losses [71 (p. 20)]. Therefore, quantitatively evaluating scientific studies related to maritime cybersecurity and conducting a comprehensive analysis of the existing academic framework has become crucial for the more effective development of cybersecurity strategies in the maritime sector and for grounding sector-specific policies on scientific evidence. In this

context, this study aims to conduct a comprehensive analysis of the scientific literature focusing on maritime cybersecurity and to reveal the development dynamics of scientific production in this field. Accordingly, searches were conducted based on the criteria defined in the study, and 248 publications obtained from the Web of Science database were analyzed using the R program. The key findings and evaluations derived from the analysis are as follows:

- It has been observed that the number of publications in this field has significantly increased, particularly from 2018 onwards. This increase indicates a growing interest in cybersecurity issues within the academic community of the maritime sector. Similarly, a study conducted by [27] reveals that publications in this area were concentrated between 2016 and 2020, supporting the findings of this study.
- "Collision-avoidance navigation" has been identified as a significant sub-theme within the scientific studies in this field. In their studies, [25] and [19] found that collision prevention stands out in cybersecurity applications in the maritime sector. Additionally, issues such as software malfunctions, hazard assessment, and human-machine interaction have also gained attention. Therefore, it is believed that alongside the development of collision prevention systems for autonomous ships, there is a need for cybersecurity research on software malfunctions and hazard assessment. Based on these findings, it is recommended that maritime operators invest in developing resilient software validation protocols and hazard response simulations that can be integrated into ship automation systems.
- The topics of "Ships performance" and "automation" have low centrality in this field. Giving more attention to research on these topics would contribute to broadening their academic scope beyond a narrow interest. On the other hand, the topics of "Cyber" and "authentication AIS" are emerging areas in maritime cybersecurity research. [28] highlighted that manipulating GPS and AIS signals should be a focus within the scope of cyber threats. This finding supports the results of this study. To address these emerging threats, international maritime authorities should prioritize the implementation of authentication protocols for AIS and GPS signals and promote the development of tamper-resistant navigation systems.
- Scientific studies in this field concentrate on cybersecurity and risk management in autonomous ships, cybersecurity in port and maritime infrastructures, types of cyberattacks, and threats in the maritime sector. It has been observed that the studies in the maritime field aim to identify security vulnerabilities, analyze potential threats, and develop effective security solutions. In particular, studies highlighting the security vulnerabilities in critical technologies such as autonomous ships, electronic chart displays and information systems, and automatic identification systems have been identified as prominent. In this regard, it is crucial for maritime institutions to carry out regular vulnerability assessments of critical onboard systems and to implement continuous cybersecurity training for personnel. Furthermore, developing real-time monitoring systems that utilize machine learning for anomaly detection could significantly reduce response times to cyber incidents.
- Norway, the United Kingdom, and the United States have had the highest scientific productivity in this field. Similarly, [22] and [19] highlight that the United States and Norway are leading countries in terms of the number of scientific publications in this area. Developing countries, such as those in Africa, South America, and South Asia, show low levels of collaboration in this field. It is believed that cybersecurity issues in the maritime sector are not sufficiently prioritized in these regions, and these countries are at a high level of risk from cyber threats. International cooperation programs should be launched to mitigate this gap, focusing on knowledge transfer, infrastructure development, and workforce training in developing countries.
- The literature highlights the lack of international standards as a challenge in addressing cybersecurity issues in the maritime sector. Therefore, stakeholders such as the International Maritime Organization (IMO) and national maritime authorities should work together to develop standardized cybersecurity regulations that are mandatory, periodically updated, and aligned with technological advancements. In the future, establishing and implementing these standards will be critical to enhancing security within the sector.
- Research in the literature is generally based on theoretical models, with a noted lack of studies focused on real-world applications. It has been identified that future studies in this field should include more analysis of human-machine interactions, the use of blockchain technology for cybersecurity in the maritime sector, and further experimental research on risk analysis for autonomous systems. As a concrete step forward, collaborative pilot projects between academia and industry should be encouraged to test theoretical models in operational maritime environments. This would help validate research outcomes and facilitate their practical adoption.

In conclusion, the acceleration of the digitalization process in the maritime sector has made cybersecurity issues more critical, both academically and practically. However, for the field to mature further, more studies are needed to ensure the applicability of theoretical frameworks and models to real-world scenarios and develop innovative solution proposals. The findings of this study suggest the need for a multi-layered cybersecuri-

ty strategy involving technical safeguards, personnel training, and regulatory frameworks. Studies conducted in this field will not only enhance operational efficiency within the sector but will also play a significant role in ensuring the security of the global supply chain. Moving forward, maritime organizations, regulators, and researchers must jointly develop actionable roadmaps that translate academic knowledge into sector-wide protective measures. Future scientific research in this area will contribute to integrating theoretical approaches into practical applications.

This study contributes to understanding the dynamics of scientific production in maritime cybersecurity; however, it also has certain limitations. Firstly, the analysis is limited to publications indexed in the Web of Science database. This may have led to the exclusion of relevant studies available in other databases, such as Scopus and ProQuest, potentially restricting the comprehensiveness of the dataset. In addition, although bibliometric methods provide valuable insights into publication trends, influential authors, and thematic structures, they may not fully reflect individual studies' practical impact or content depth. Furthermore, the dataset used in this study is based on records retrieved as of December 2024. Publications added to the database after this date may lead to different analyses and findings in the future. Considering these limitations, caution should be exercised when generalizing the results, and future research is encouraged to expand the dataset and adopt a mixed-methods approach that integrates both quantitative and qualitative analyses to offer a more holistic perspective on the field.

5 Recommendations for Future Research

Based on the findings, the following recommendations for future studies on cybersecurity applications in the maritime sector can be outlined:

- Since collisions in the maritime sector are among the most serious accidents, further research on cybersecurity applications could be conducted during the development process of collision avoidance systems in autonomous ships. Future studies could explore how real-time threat detection algorithms can be integrated with navigational decision-making in autonomous systems, ensuring both safety and cyber resilience.
- The topics of "Cyber" and "authentication AIS" are in the development stage within maritime cybersecurity research. This presents opportunities for researchers who wish to conduct more comprehensive and innovative studies in this field. For example, designing end-to-end encrypted AIS communication protocols or AI-driven authentication systems could offer practical and novel contributions to vessel identity verification and tracking integrity.
- Future research could focus on examining legal regulations related to maritime cybersecurity, analyzing the policies of international organizations in this area, and developing regulatory frameworks for the sector. In addition, comparative policy analysis between regulatory approaches adopted by different maritime nations may reveal best practices and inform the development of harmonized global standards.
- Systematic literature reviews focusing on various subtopics related to maritime cybersecurity applications, such as ship networks, sensor systems, electronic chart systems, and the use of blockchain technology, will contribute to the more effective development of strategies in this field and support grounding sector-specific policies on scientific evidence. Moreover, these reviews could be complemented by meta-analyses that evaluate the effectiveness of different technical solutions in reducing attack surfaces and enhancing system resilience.
- In research conducted in this field, collaboration among researchers has remained limited. Similarly, [20] emphasizes the need for enhancing international collaboration. Therefore, academic collaboration networks among authors from different countries should be strengthened, and academic programs and scientific projects that bring researchers together should be encouraged to increase interdisciplinary knowledge sharing.
- In particular, access to information and communication technologies in developing countries should be improved, and cybersecurity awareness should be increased. International educational programs, academic research, and industry collaborations involving countries such as the United Kingdom, the United States, and Norway should be encouraged to achieve this.

Funding: The research presented in the manuscript received no external funding.

Acknowledgments: This paper was presented as a proceedings paper at the V. BİLSEL International Ahlat Scientific Research Congress.

References

[1] Dui, H., Zheng, X., & Wu, S. (2021). Resilience analysis of maritime transportation systems based on importance measures. *Reliability Engineering & System Safety*, *209*, 107461. https://doi.org/10.1016/j.ress.2021.107461

[2] Fratila (Adam), A., Gavril (Moldovan), I. A., Nita, S. C., & Hrebenciuc, A. (2021). The Importance of Maritime Transport for Economic Growth in the European Union: A Panel Data Analysis. *Sustainability*, *13*(14), Article 14. https://doi.org/10.3390/su13147961

[3] UNCTAD. (2024). *Review of Maritime Transport*. https://unctad.org/system/files/official-document/rmt2024_en.pdf

[4] Kaštelan, N., Vidan, P., Assani, N., & Miličević, M. (2024). Digital Horizon: Assessing Current Status of Digitalization in Maritime Industry. *Transactions on Maritime Science*, *13*(1). https://doi.org/10.7225/toms.v13.n01.w13

[5] Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, *37*, 100526. https://doi.org/10.1016/j.ijcip.2022.100526

[6] Bocayuva, M. (2021). Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic. *WMU Journal of Maritime Affairs*, *20*(2), 173–192. https://doi.org/10.1007/s13437-021-00240-4

[7] Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, *45*, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058

[8] Dryad Global. (2025). https://safety4sea.com/wp-content/uploads/2025/01/DryadGlobal-Maritime-Trends-for-2025-2025_01.pdf

[9] Svilicic, B., Kamahara, J., Rooks, M., & Yano, Y. (2019). Maritime Cyber Risk Management: An Experimental Ship Assessment. *The Journal of Navigation*, *72*(5), 1108–1120. https://doi.org/10.1017/S0373463318001157

[10] Svilicic, B., Kristić, M., Žuškin, S., & Brčić, D. (2020). Paperless ship navigation: Cyber security weaknesses. *Journal of Transportation Security*, *13*(3–4), 203–214. https://doi.org/10.1007/s12198-020-00222-2

[11] Tam, K., & Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, *18*(1), 129–163. https://doi.org/10.1007/s13437-019-00162-2

[12] Androjna, A., Perkovič, M., & Pavić, I. (2021). Cyber Security Challenges for Safe Navigation at Sea. *14th Annual Baška GNSS Conference: Technologies, Techniques and Applications Across PNT and The 1st Workshop on Smart, Blue and Green Maritime Technologies*, 47–62. https://www.researchgate.net/profile/David-Brcic/publication/358671686_Proceedings_14th_Annual_Baska_GNSS_Conference_Technologies_Techniques_and_Applications_Across_PNT_and_The_1st_Workshop_on_Smart_Blue_and_Green_Maritime_Technologies/links/620e72eeeb735c508adb3928/Proceedings-14th-Annual-Baska-GNSS-Conference-Technologies-Techniques-and-Applications-Across-PNT-and-The-1st-Workshop-on-Smart-Blue-and-Green-Maritime-Technologies.pdf#page=48

[13] Amro, A., & Gkioulos, V. (2022). From Click to Sink: Utilizing AIS for Command and Control in Maritime Cyber Attacks. In V. Atluri, R. Di Pietro, C. D. Jensen, & W. Meng (Eds.), *Computer Security – ESORICS 2022* (pp. 535–553). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-17143-7_26

[14] Jacq, O., Boudvin, X., Brosset, D., Kermarrec, Y., & Simonin, J. (2018). Detecting and Hunting Cyberthreats in a Maritime Environment: Specification and Experimentation of a Maritime Cybersecurity Operations Centre. *2018 2nd Cyber Security in Networking Conference (CSNet)*, 1–8. https://doi.org/10.1109/CSNET.2018.8602669

[15] Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers & Security*, *103*, 102196. https://doi.org/10.1016/j.cose.2021.102196

[16] Amro, A., & Gkioulos, V. (2023). Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. *International Journal of Information Security*, *22*(1), 249–288. https://doi.org/10.1007/s10207-022-00638-y

[17] Meland, P. Há., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A Retrospective Analysis of Maritime Cyber Security Incidents. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *15*(3), 519–530. https://doi.org/10.12716/1001.15.03.04

[18] Meland, P. H., Nesheim, D. A., Bernsmed, K., & Sindre, G. (2022). Assessing cyber threats for storyless systems. *Journal of Information Security and Applications*, *64*, 103050. https://doi.org/10.1016/j.jisa.2021.103050

[19] Chaal, M., Ren, X., BahooToroody, A., Basnet, S., Bolbot, V., Banda, O. A. V., & Gelder, P. V. (2023). Research on risk, safety, and reliability of autonomous ships: A bibliometric review. *Safety Science*, *167*, 106256. https://doi.org/10.1016/j.ssci.2023.106256

[20] Symes, S., Blanco-Davis, E., Graham, T., Wang, J., & Shaw, E. (2024). Cyberattacks on the Maritime Sector: A Literature Review. *Journal of Marine Science and Application*, *23*(4), 689–706. https://doi.org/10.1007/s11804-024-00443-0

[21] Drummond, B. M., & Machado, R. C. S. (2021). Cyber Security Risk Management for Ports—A Systematic Literature Review. *2021 International Workshop on Metrology for the Sea; Learning to Measure Sea Health Parameters (MetroSea)*, 406–411. https://doi.org/10.1109/MetroSea52177.2021.9611569

[22] De Albuquerque, C. E. P., Machado, R. C. S., De Sa, A. O., & De Toledo, C. R. B. (2022). Bibliometric Analysis on Cyber-Attacks in Naval Sensors and Systems. *2022 IEEE International Workshop on Metrology for the Sea; Learning to Measure Sea Health Parameters (MetroSea)*, 474–478. https://doi.org/10.1109/MetroSea55331.2022.9950939

[23] Martínez, F., Sànchez, L. E., Santos-Olmo, A., Rosado, D. G., & Fernàndez-Medina, E. (2024). Maritime cybersecurity: Protecting digital seas. *International Journal of Information Security*, *23*(2), 1429–1457. https://doi.org/10.1007/s10207-023-00800-0

[24] Larsen, M. H., & Lund, M. S. (2021). Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review. *IEEE Access*, *9*, 144895–144905. IEEE Access. https://doi.org/10.1109/ACCESS.2021.3122433

[25] Li, Z., Zhang, D., Han, B., & Wan, C. (2023). Risk and reliability analysis for maritime autonomous surface ship: A bibliometric review of literature from 2015 to 2022. *Accident Analysis & Prevention*, *187*, 107090. https://doi.org/10.1016/j.aap.2023.107090

[26] Erbas, M., Khalil, S. M., & Tsiopoulos, L. (2024). Systematic literature review of threat modeling and risk assessment in ship cybersecurity. *Ocean Engineering*, *306*, 118059. https://doi.org/10.1016/j.oceaneng.2024.118059

[27] Harish, A. V., Tam, K., & Jones, K. (2024). Literature review of maritime cyber security: The first decade. *Maritime Technology and Research*, *7*(2), 273805. https://doi.org/10.33175/mtr.2025.273805

[28] Yu, H., Meng, Q., Fang, Z., & Liu, J. (2023). Literature review on maritime cybersecurity: State-of-the-art. *Journal of Navigation*, *76*(4–5), 453–466. https://doi.org/10.1017/S0373463323000164

[29] Büyükkıdık, S. (2022). A Bibliometric Analysis: A Tutorial for the Bibliometrix Package in R Using IRT Literature. *Journal of Measurement and Evaluation in Education and Psychology*, *13*(3), Article 3.

[30] Guleria, D., & Kaur, G. (2021). Bibliometric analysis of ecopreneurship using VOSviewer and RStudio Bibliometrix, 1989–2019. *Library Hi Tech*, *39*(4), 1001–1024. https://doi.org/10.1108/LHT-09-2020-0218

[31] Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, *133*, 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

[32] Passas, I. (2024). Bibliometric analysis: The main steps. *Encyclopedia*, *4*(2), Article 2.

[33] Gutiérrez-Salcedo, M., Martínez, M. Á., Moral-Munoz, J. A., Herrera-Viedma, E., & Cobo, M. J. (2018). Some bibliometric procedures for analyzing and evaluating research fields. *Applied Intelligence*, *48*(5), 1275–1287. https://doi.org/10.1007/s10489-017-1105-y

[34] Zerbini, C., Aiolfi, S., Bellini, S., Luceri, B., & Vergura, D. T. (2022). Mobile shopping behavior: A bibliometric analysis. *Sinergie Italian Journal of Management*, *40*(2), Article 2. https://doi.org/10.7433/s118.2022.11

[35] Derviş, H. (2019). Bibliometric analysis using bibliometrix an R package. *Journal of Scientometric Research*, *8*(3), 156–160.

[36] Rusydiana, A. S. (2021). Bibliometric analysis of journals, authors, and topics related to COVID-19 and Islamic finance listed in the Dimensions database by Biblioshiny. *Science Editing*, *8*(1), 72–78. https://doi.org/10.6087/kcse.232

[37] Ammar, M., & Khan, I. A. (2024). *Cyber Attacks on Maritime Assets and their Impacts on Health and Safety Aboard: A Holistic View* (arXiv:2407.08406). arXiv. https://doi.org/10.48550/arXiv.2407.08406

[38] Aşan, C. (2024). Developing a measurement scale to assess the perception of cybersecurity among employees in the maritime industry. *Journal of Naval Sciences and Engineering*, *20*(2), Article 2. https://doi.org/10.56850/jnse.1485985

[39] Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2020). Modelling Shipping 4.0: A Reference Architecture for the Cyber-Enabled Ship. In N. T. Nguyen, K. Jearanaitanakij, A. Selamat, B. Trawiński, & S. Chittayasothorn (Eds.), *Intelligent Information and Database Systems* (pp. 202–217). Springer International Publishing. https://doi.org/10.1007/978-3-030-42058-1_17

[40] Zhang, X., Wang, C., Jiang, L., An, L., & Yang, R. (2021). Collision-avoidance navigation systems for Maritime Autonomous Surface Ships: A state of the art survey. *Ocean Engineering*, *235*, 109380. https://doi.org/10.1016/j.oceaneng.2021.109380

[41] Kang, Y.-T., Chen, W.-J., Zhu, D.-Q., & Wang, J.-H. (2021). Collision avoidance path planning in multi-ship encounter situations. *Journal of Marine Science and Technology*, *26*(4), 1026–1037. https://doi.org/10.1007/s00773-021-00796-z

[42] Türkistanli, T. T., & Kuleyin, B. (2022). Game-based learning for better decision-making: A collision prevention training for maritime transportation engineering students. *Computer Applications in Engineering Education*, *30*(3), 917–933. https://doi.org/10.1002/cae.22494

[43] Namgung, H. (2021). Local Route Planning for Collision Avoidance of Maritime Autonomous Surface Ships in Compliance with COLREGs Rules. *Sustainability*, *14*(1), 198. https://doi.org/10.3390/su14010198

[44] Zhang, D., Ma, H., Chen, L., Yuan, X., & Fan, L. (2021). Cooperative collision avoidance study of Maritime Autonomous Surface Ship. *2021 6th International Conference on Transportation Information and Safety (ICTIS)*, 908–916. https://doi.org/10.1109/ICTIS54573.2021.9798577

[45] Rodríguez-Soler, R., Uribe-Toril, J., & De Pablo Valenciano, J. (2020). Worldwide trends in the scientific production on rural depopulation, a bibliometric analysis using bibliometrix R-tool. *Land Use Policy*, *97*, 104787. https://doi.org/10.1016/j.landusepol.2020.104787

[46] Algantürk Light, D. (2019). Siber Tehlikelerin Denizcilik Sektörüne Etkisi. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, *25*(2), Article 2. https://doi.org/10.33433/maruhad.665513

[47] NORMA Cyber. (2025, January 26). *More About NORMA Cyber*. https://www.normacyber.no/en/moreabout

[48] UK Government. (2022, August 15). *New maritime security strategy to target latest physical and cyber threats*. https://www.gov.uk/government/news/new-maritime-security-strategy-to-target-latest-physical-and-cyber-threats

[49] Library of Congress. (2022, March 1). *Strengthening American Cybersecurity Act of 2022*. https://www.congress.gov/bill/117th-congress/senate-bill/3600

[50] Peng, P., Xie, X., Claramunt, C., Lu, F., Gong, F., & Yan, R. (2025). Bibliometric analysis of maritime cybersecurity: Research status, focus, and perspectives. *Transportation Research Part E: Logistics and Transportation Review*, *195*, 103971. https://doi.org/10.1016/j.tre.2025.103971

[51] Cary, D. (2021, July). *China's National Cybersecurity Center: A Base for Military-Civil Fusion in the Cyber Domain*. Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/chinas-national-cybersecurity-center/

[52] Creemers, R., Webster, G., & Triolo, P. (2018, June 29). *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

[53] Statista. (2025, January 26). *Cybersecurity—United States*. https://www.statista.com/outlook/tmo/cybersecurity/united-states

[54] Statista. (2025, January 26). *Cybersecurity – China*. https://www.statista.com/outlook/tmo/cybersecurity/china

[55] de la Peña Zarzuelo, I., Freire Soeane, M. J., & López Bermúdez, B. (2020). Industry 4.0 in the port and maritime industry: A literature review. *Journal of Industrial Information Integration*, *20*, 100173. https://doi.org/10.1016/j.jii.2020.100173

[56] Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship

systems. *Safety Science*, *131*, 104908. https://doi.org/10.1016/j.ssci.2020.104908

[57] Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information*, *13*(1), Article 1. https://doi.org/10.3390/info13010022

[58] Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2023). A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2677–2690. https://doi.org/10.1109/TITS.2022.3164678

[59] Androjna, A., Perkovič, M., Pavic, I., & Mišković, J. (2021). AIS Data Vulnerability Indicated by a Spoofing Case-Study. *Applied Sciences*, *11*(11), Article 11. https://doi.org/10.3390/app11115015

[60] Kessler, G. C., Craiger, J. P., & Haass, J. C. (2018). A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *12*(3), 429–437. https://doi.org/10.12716/1001.12.03.01

[61] Akdağ, M., Solnør, P., & Johansen, T. A. (2022). Collaborative collision avoidance for Maritime Autonomous Surface Ships: A review. *Ocean Engineering*, *250*, 110920. https://doi.org/10.1016/j.oceaneng.2022.110920

[62] Abaei, M. M., Hekkenberg, R., & BahooToroody, A. (2021). A multinomial process tree for reliability assessment of machinery in autonomous ships. *Reliability Engineering & System Safety*, *210*, 107484. https://doi.org/10.1016/j.ress.2021.107484

[63] Carreras Guzman, N. H., Wied, M., Kozine, I., & Lundteigen, M. A. (2020). Conceptualizing the key features of cyber-physical systems in a multi-layered representation for safety and security analysis. *Systems Engineering*, *23*(2), 189–210. https://doi.org/10.1002/sys.21509

[64] Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. *Journal of Marine Science and Engineering*, *8*(10), Article 10. https://doi.org/10.3390/jmse8100776

[65] Caprolu, M., Pietro, R. D., Raponi, S., Sciancalepore, S., & Tedeschi, P. (2020). Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. *IEEE Communications Magazine*, *58*(6), 90–96. https://doi.org/10.1109/MCOM.001.1900632

[66] Bolbot, V., Theotokatos, G., Wennersberg, L., Faivre, J., Vassalos, D., Boulougouris, E., Jan Rødseth, Ø., Andersen, P., Pauwelyn, A.-S., & Van Coillie, A. (2023). A novel risk assessment process: Application to an autonomous inland waterways ship. *Proceedings of the Institution of Mechanical Engineers, Part O*, *237*(2), 436–458. https://doi.org/10.1177/1748006X211051829

[67] de la Peña Zarzuelo, I. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. *Transport Policy*, *100*, 1–4. https://doi.org/10.1016/j.tranpol.2020.10.001

[68] Chae, C.-J., Kim, M., & Kim, H.-J. (2020). A Study on Identification of Development Status of MASS Technologies and Directions of Improvement. *Applied Sciences*, *10*(13), Article 13. https://doi.org/10.3390/app10134564

[69] Hareide, O. S., Jøsok, Ø., Lund, M. S., Ostnes, R., & Helkala, K. (2018). Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *The Journal of Navigation*, *71*(5), 1025–1039. https://doi.org/10.1017/S0373463318000164

[70] Park, C., Kontovas, C., Yang, Z., & Chang, C.-H. (2023). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management*, *235*, 106480. https://doi.org/10.1016/j.ocecoaman.2023.106480

[71] Kala, N., & Balakrishnan, M. (2019). Cyber Preparedness in Maritime Industry. *International Journal of Scientific and Technical Advancements*, *5*(2), 19–28.